UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF PENNSYLVANIA
PHILADELPHIA DIVISION

BARRY K. GRAHAM, ANGELA MORGAN, and STEPHEN MOTKOWICZ, individually and on behalf of all others similarly situated, Plaintiffs, v. UNIVERSAL HEALTH SERVICES, INC., Defendant.	Case No.: 2:20-cv-05375 **AMENDED COMPLAINT** **CLASS ACTION** **JURY TRIAL DEMANDED**

Plaintiffs, Barry K. Graham ("Graham"), Angela Morgan ("Morgan"), and Stephen Motkowicz ("Motkowicz") (collectively "Plaintiffs"), individually and on behalf of the Class defined below of similarly situated persons, bring this Class Action Complaint and allege the following against Defendant Universal Health Services, Inc. ("Defendant"), based upon personal knowledge with respect to Plaintiffs' self and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters:

NATURE OF THE ACTION

1. Plaintiffs bring this class action against Defendant for its failure to properly secure and safeguard protected health information as defined by the Health Insurance Portability and Accountability Act ("HIPAA"), medical information, and other personally identifiable information (collectively, "PHI"), for failing to comply with industry standards for the protection of that PHI, as well as failing to provide accurate and adequate notice to Plaintiffs and other Class Members that their PHI had been compromised and precisely what types of information was compromised. Plaintiffs seek, among other things, orders requiring Defendant to fully and accurately disclose the nature of the information that has been compromised and to adopt

reasonably sufficient security practices and safeguards to prevent incidents like the disclosure in the future.

2. On or about September 28, 2020, Defendant announced that its "IT Network across Universal Health Services (UHS) facilities is currently offline, due to an IT security issue."[1] However, an individual familiar with the company's response efforts said the attack (not issue) "looks and smells like ransomware," (the "Data Breach").[2]

3. Defendant has more than 400 locations, primarily in the United States, and in 2019 generated net revenues of $11.4 billion—an increase of 5.6% over the prior fiscal year.[3]

4. In 2019, Defendant expended $634 million investing in equipment, facility expansions and renovations.[4]

5. As a result of Defendant's failure to implement and follow appropriate security procedures, Plaintiffs' and Class Members' PHI has been compromised. Plaintiffs and Class Members now face a substantial increased risk of identity theft. Consequently, Defendant's current and former customers have had to spend, and will continue to spend, significant time and money in the future to protect themselves due to Defendant's failures.

6. Additionally, as a result of Defendant's failures, Plaintiffs and Class Members received only a diminished value of the services they paid Defendant to provide. Defendant expressly represented it would maintain the confidentiality of Plaintiffs' and Class Members' PHI

---

1 *Statement from Universal Health Services*, Universal Health Services, Inc. (Sep. 28, 2020), *available at*: https://www.uhsinc.com/statement-from-universal-health-services/ (the "UHS Statement")

2 Kevin Collier, *Major hospital system hit with cyberattack, potentially largest in U.S. history*, NBCNews (Sep. 28, 2020), *available at*: https://www.nbcnews.com/tech/security/cyberattack-hits-major-u-s-hospital-system-n1241254

3 *2019 Company Overview*, Universal Health Services, Inc., *available at*: https://www.uhsinc.com/wp-content/uploads/2020/04/UHS_2019-CompanyOverview2_.pdf

4 *Id.*

obtained through course of treatment.[5]

7. Accordingly, Plaintiffs, individually and on behalf of all others similarly situated, allege claims for negligence, invasion of privacy, breach of implied contract, unjust enrichment, breach of fiduciary duty, and breach of confidence.

JURISDICTION AND VENUE

8. This Court has jurisdiction over this action pursuant to the Class Action Fairness Act 28 U.S.C. § 1332(d) ("CAFA"), because the aggregate amount in controversy exceeds $5,000,000, exclusive of interests and costs, there are more than 100 Class Members, and at least one class Member is a citizen of a state different from Defendant.

9. This Court has personal jurisdiction over Defendant because Defendant maintains its principal place of business in this District, regularly conducts business in this District, and is authorized to and does conduct substantial business in this District.

10. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(1) & (2) because Defendant's principal place of business is in this District and a substantial part of the events or omissions giving rise to this action occurred in this District.

PARTIES

11. Plaintiff Barry K. Graham is a citizen and resident of Sarasota, Florida.

12. At all times relevant to this Complaint, Plaintiff was a customer/patient of Defendant, whose PHI was disclosed without his authorization to an unknown third party as a result of the Data Breach.

13. Plaintiff Angela Morgan is a citizen and resident of Athens, Tennessee.

14. At all times relevant to this Complaint, Plaintiff Graham was a customer/patient of

[5] *UHS Privacy Policies*, Universal Health Services, Inc. https://www.uhsinc.com/compliance-and-ethics/uhs-privacy-policies/ (the "UHS Privacy Policies")

Defendant, whose PHI was disclosed without her authorization to an unknown third party as a result of the Data Breach.

15. Plaintiff Stephen Motkowicz is a citizen and resident of Manatee County, Florida.

16. At all times relevant to this Complaint, Plaintiff Motkowicz was a customer/patient of Defendant, whose PHI was disclosed without his authorization to an unknown third party as a result of the Data Breach.

17. Defendant Universal Health Services, Inc., is a publicly-traded Delaware corporation with its principal address at 367 South Gulph Road, King of Prussia, Pennsylvania 19406, according to its most-recent filings with the Securities and Exchange Commission. It is listed on the New York Stock Exchange ("NYSE") under the symbol "UHS".

18. Defendant is one of the largest healthcare companies in the United States, providing healthcare services to millions of people in a majority of the United States.

FACTUAL BACKGROUND

A. Security Breaches Lead to Identity Theft

19. In June 2007, the United States Government Accountability Office reported that identity thieves use identifying data, such as Social Security Numbers, to open financial accounts, intercept government benefits, and incur charges and credit in a person's name.[6] The GAO affirmed this type of identity theft is the most harmful because it may take some time for the victim to become aware of the theft and can adversely impact the victim's credit rating. In addition, the GAO Report informs that victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records…[and their] good name."[7]

---

[6] *Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown*, GAO (June 2007), *available at* https://www.gao.gov/new.items/d07737.pdf (the "GAO Report")

[7] *Id.*

20. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[8] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[9]

21. The FTC acknowledges that identity theft victims must spend countless hours and large amounts of money repairing the impact to their good name and credit record.[10] Identity thieves use stolen PHI such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[11]

22. Once PHI is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

23. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change.

24. The Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later.[12] This time lag

---

8 17 C.F.R. § 248.201 (2013).

9 *Id.*

10 *Guide for Assisting Identity Theft Victims*, FTC (Sep. 2013), *available at*: https://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf (the "FTC Guide").

11 FTC Guide, *supra* n.10.

12 *Identity Theft and Your Social Security Number*, Social Security Administrative *available at* http://www.ssa.gov/pubs/EN-05-10064.pdf.

between when harm occurs versus when it is discovered, and also between when PHI is stolen and when it is used, compounds an identity theft victim's ability to detect and address the harm.

25. According to the GOA, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[13]

26. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

27. Stolen PII is often trafficked on the "dark web," a part of the Internet that is not accessible via traditional search engines. When malicious actors infiltrate companies and the PHI that those companies store, that stolen information often ends up on the dark web because the malicious actors are motivated by the monetary value of that PHI, including buying and selling it in dark web marketplaces.[14]

28. For example, when the U.S. Department of Justice announced its seizure of AlphaBay in 2017, AlphaBay had more than 350,000 listings, many of which concerned stolen or fraudulently-obtained documents that could be used to assume another person's identity. Other

---

[13] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at* http://www.gao.gov/new.items/d07737.pdf.

[14] *Shining a Light on the Dark Web with Identity Monitoring*, IdentityForce, Dec. 28, 2020, *available at:* https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring.

marketplaces, similar to the now-defunct AlphaBay, "are awash with [personal information] belonging to victims from countries all over the world. One of the key challenges in protecting [personal information] online is its pervasiveness. As data breaches in the news continue to show, [personal information] about employees, customers, and the public is housed in all kinds of organizations, and the increasing digital transformation of today's businesses only broadens the number of potential sources for hackers to target."[15]

29. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[16]

30. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security Number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

31. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[17]

---

[15] *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, Armor, April 3, 2018, *available at:* https://www.armor.com/resources/blog/stolen-pii-ramifications-identity-theft-fraud-dark-web/

[16] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at* http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

[17] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at* http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.

32. With access to a person's PHI, criminals are capable of conducting myriad nefarious actions in addition to emptying a victim's bank account. Identity thieves also commit various types of government fraud, such as: obtaining a driver's license or official identification card in the victim's name with the thief's picture; using the victim's name and Social Security number to steal government benefits; and filing a fraudulent tax return using the victim's information. Worse, identity thieves may obtain a job using a victim's Social Security number, rent a house, receive medical services in the victim's name, or give the victim's information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[18]

33. PHI is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for a number of years.[19] As a result of large-scale data breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers, Social Security numbers, healthcare information, and other PHI directly on various Internet websites making the information publicly available. These networks and markets consist of hundreds of thousands, if not millions, of nefarious actors who view and access the PHI.

34. In one study from 2010, researchers found hundreds of websites displaying stolen personal information, including PHI. Strikingly, none of these websites were blocked by Google's safeguard filtering mechanism—the "Safe Browsing list." The study concluded:

> It is clear from the current state of the credit card black-market that cyber criminals can operate much too easily on the Internet. They are not afraid to put out their email addresses, in some cases phone numbers and other credentials in their advertisements. It seems that the black market for cyber criminals is not underground at all. In fact, it's very "in your face."[20]

---

18 FTC Guide, *supra* n.10.
19 FTC Guide, *supra* n.10.
20 *The "Underground" Credit Card Blackmarket*, StopTheHacker, *available at:* http://credit-help.pro/credit/59241

35. In another report about health-care related identity theft fraud sponsored by Experian indicated that the "average total cost to resolve an identity theft-related incident…came to about $20,000." Further, a majority of the victims were forced to pay out-of-pocket costs for health care they did not receive in order to restore coverage. Moreover, almost 50 percent of the victims lost their health care coverage as a result of the incident, while nearly one-third said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Indeed, data breaches and identity theft have a crippling effect on individuals and detrimentally impact the entire economy as a whole.[21]

36. That an entity is infected with ransomware does not mean the information at issue was not exfiltrated. In fact, ransomware operations have evolved with data leak threats, extortion, and indeed exfiltration, leaking the sensitive and confidential information to the dark web.[22]

B. Defendant Obtains, Collects, and Stores Plaintiffs' and Class Members' PHI

37. Defendant is one of the largest healthcare companies in North America, operating approximately 400 locations. As one of the largest healthcare companies Defendant collects, stores, and maintains a massive amount of PHI on its customers and/or patients.

38. As a condition of providing healthcare to customers/patients, Defendant requires that its customers/patients entrust it with PHI. In its ordinary course of business, Defendant maintains PHI, including the name, address, zip code, date of birth, Social Security number, medical diagnoses, insurance information, and other sensitive and confidential information for current and former customers/patients.

---

[21] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010) https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/

[22] *See, e.g.*, CrowdStrike, *Double Trouble: Ransomware with Data Leak Extortion* (Sep. 24, 2020) https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1/; CrowdStrike, *Double Trouble: Ransomware with Data Leak Extortion, Part 2* (Oct. 6, 2020) https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-2/

39. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and the Class Members' PHI, Defendant assumed legal and equitable duties to those individuals. Defendant knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' PHI from disclosure. At all relevant time, Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their PHI.

40. Plaintiffs and the Class Members, as current and former customers/patients, relied on Defendant to keep their PHI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

C. Defendant's Privacy Policy and Agreements to Keep PHI Confidential

41. Defendant represented to Plaintiffs and Class Members that it would protect their PHI. Through its Privacy Policies, Defendant provides patients/customers with myriad policies concerning those customers/patients' confidentiality and privacy rights.[23]

42. Defendant created these policies, representations, and requirements, and publicly advertised them on its website as a means of increasing the value of its relationships with patients/customers, thus allowing it to charge consumers higher rates under the guise of enhanced security and information security practices.

D. The Data Breach

43. On September 28, 2020, Defendant took the entirety of its IT network offline, resulting to paper-based record keeping.[24] This ordinarily would not be reported to the news and public at large; however, a source familiar with the response and removal of the IT network's online status revealed that it "look[ed] and smell[ed] like ransomware." To date, Defendant has provided scant details of the Data Breach, and although it has represented there was "no indication

[23] UHS Privacy Policies, *supra* n.5.
[24] UHS Statement, *supra* n.1.

that any patient or employee data was accessed, copied, or misused," Defendant provides no factual basis or details of the investigation, the extent of any review, or any further assurances to customers/patients beyond the conclusory, vague statement from October 12, 2020.[25]

44. Defendant took no action to promptly notify its patients/customers that might be affected by the Data Breach.

45. Defendant, knowing that PHI is subject to the strict privacy and security protections of HIPAA, and other standards and regulations, delayed and otherwise failed to properly and timely provide notice to Plaintiffs and Class Members regarding the compromised PHI.

46. Defendant has acknowledged the sensitive and confidential nature of the PHI. To be sure, collection, maintaining, and protecting PHI is vital to many of Defendant's business purposes. Defendant has acknowledged through conduct and statements that the misuse or inadvertent disclosure of PHI can pose major privacy and financial risks to impacted individuals, and that under state law they may not disclose and must take reasonable steps to protect PHI from improper release or disclosure. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgment of its duties to keep PHI private and secure, Defendant failed to take appropriate steps to protect the PHI of Plaintiffs and Class Members from being compromised.

47. The ramifications of Defendant's failure to keep its customers/patients' PHI secure are long lasting and severe.

48. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, say, credit card information in a large retailer data breach such as those that occurred at Target and Home Depot; there, victims could cancel or close

[25] *Statement from Universal Health Services*, Universal Health Services, Inc. (Oct. 12, 2020), *available at*: https://www.uhsinc.com/statement-from-universal-health-services/

credit and debit card accounts. The information compromised in the Data Breach, however, is impossible to "close" and difficult, if not impossible, to change—Social Security number, name, date of birth, address, medical information, and other PHI.

49. Defendant designed and implemented its policies and procedures regarding the security of PHI. Although Defendant's most-recent published policies took effect in October 2017, these policies and procedures failed to adhere to reasonable and best industry practices in safeguarding PHI.

50. Upon information and believe, Defendant failed to effectively supervise its workforce (including both employees and independent contractors) on the policies and procedures with respect to the appropriate maintenance, use, and disclosure of PHI.

51. Defendant's collective failure to safeguard Plaintiffs' and Class Members' PHI resulted in the exposure of that PHI.

52. As some of Defendant's patients/customers, Plaintiffs provided Defendant with their accurate PHI. Upon information and belief, Defendant's IT network contained Plaintiffs' PHI. Class Members similarly provided Defendant with their PHI, and Defendant's IT network contained Class Members' PHI.

53. The affected individuals face a real, concrete, and actual risk of harm and future identity theft as the PHI contained confidential biographical and other medical information.

54. As a consequence of the Data Breach, Plaintiffs and Class Members have suffered damages by taking measures to both deter and detect identity theft. Plaintiffs and Class Members have been required to take time, which they otherwise would have dedicated to other life demands (such as work or leisure), and effort to mitigate the actual and potential impact of the Data Breach on their lives including, *inter alia*; placing "freezes" and "alerts" with credit reporting agencies,

contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports. This time has been lost forever and cannot be recaptured. In all manners of life in this country, time has constantly been recognized as compensable: indeed, for many consumers it is the way they are compensated; and even if retired from the workforce, consumers should be free of having to deal with the consequences of companies' wrongful conduct, as is the case here.

55. Without question, the PHI of Plaintiffs and Class Members, particularly their Social Security numbers, protected health information, and dates of birth, can be used for purposes of identity theft, and unfortunately, Defendant's current and former customers/patients are now, and for the rest of their lives will be, at a heightened risk of further identity theft and fraud.

E. Defendant's Data Breach Caused Plaintiffs' Injuries

56. Defendant's Data Breach caused Plaintiffs' damages.

57. Through their treatment with Defendant, Plaintiffs provided health history as well as particular PHI to which only Defendant would have access.

58. Plaintiffs never transmitted unencrypted PHI over the internet or any other unsecured source.

59. Plaintiffs store any and all documents containing their PHI in a safe and secure physical location, and destroyed any documents they receive in the mail that contain any PHI, or that may contain any information that could otherwise be used to commit identity theft.

60. Following the Data Breach, Plaintiffs' PHI has been disseminated to unauthorized third parties who are now free to exploit and misuse that PHI without any ability for Plaintiffs to recapture and erase that PHI from further dissemination—Plaintiffs' PHI is forever compromised, and this PHI was unique to the PHI Defendant improperly safeguarded.

61. But for Defendant's Data Breach, Plaintiffs would not have incurred the loss and publication of their PHI and other injuries.

62. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PHI.

63. Despite all of the publicly available knowledge of the continued compromises of PHI, Defendant's approach to maintaining the privacy of their customers/patients' PHI was lackadaisical, cavalier, reckless, or in the very least, negligent.

64. In all manners of life in this country, time has constantly been recognized as compensable, for many people it is the way they are compensated. Plaintiffs and Class Members should be free of having to deal with the consequences of Defendant's slippage.

65. Additionally, Plaintiff Motkowicz suffered financial damages in the form of increased insurance payments due to Defendant's conduct resulting in the Data Breach. Specifically, Plaintiff Motkowicz was scheduled for a procedure on September 28, 2020. On the evening of September 27, 2020, however, Plaintiff Motkowicz received a communication from Defendant informing him that a ransomware attack had infected Defendant's computer systems, and that all procedures were being cancelled. Mr. Motkowicz informed Defendant that it was imperative that the procedure be rescheduled as soon as possible, but the surgery was rescheduled approximately six (6) weeks later. The rescheduling of this procedure caused Mr. Motkowicz to continue to miss work because the nature of his medical condition required this procedure (and recovery) prior to returning to work and, because he could not return to work, his insurance lapsed and he was required to procure alternative insurance at an increased cost to him to pay for the surgery.

F. Defendant's Conduct Violates HIPAA and Industry Standard Practices

66. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PHI like the data Defendant left unguarded. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

67. Defendant's Data Breach resulted from a combination of insufficiencies that indicate Defendant failed to comply with safeguards mandated by HIPAA regulations and industry standards. First, it can be inferred from Defendant's Data Breach that Defendant either failed to implement, or inadequately implemented, information security policies or procedures prohibiting storing PHI on computers and/or information security policies or procedures in place regarding encryption or protecting PHI.

68. In addition, Defendant's Data Breach could have been prevented if Defendant implemented HIPAA mandated, industry standard policies and procedures for securely disposing of PHI when it was no longer necessary and/or had honored its obligations to their patients/customers.

69. Contributing to the problem was Defendant's failure to effectively supervise and train its employees that were in charge of designing and implementing policies and procedures on the appropriate maintenance, use, and disclosure of PHI.

70. Defendant's security failures also include, but are not limited to:

a. Failing to maintain an adequate data security system to prevent data loss;

b. Failing to mitigate the risks of a data breach and loss of data;

c. Failing to adequately catalog the location of patients/customers', including

Plaintiffs' and Class Members', digital information;

d. Failing to ensure the confidentiality and integrity of electronic protected health information Defendant creates, receives, maintains, and transmits in violation of 45 CFR 164.306(a)(1);

e. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1);

f. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

g. Failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 CFR 164.308(a)(6)(ii);

h. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2);

i. Failing to protect against any reasonably-anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 CFR 164.306(a)(3);

j. Failing to ensure compliance with HIPAA security standard rules by its workforce in violation of 45 CFR 164.306(a)(94);

k. Impermissibly and improperly using and disclosing protected health information

that is and remains accessible to unauthorized persons in violation of 45 CFR 164.502, *et seq.*;

l. Failing to effectively train all members of its workforce (including independent contractors) on the policies and procedures with respect to protected health information as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of protected health information in violation of 45 CFR 164.530(b) and 45 CFR 164.308(a)(5); and

m. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard protected health information, in compliance with 45 CFR 164.530(c).

71. In light of the foregoing, Defendant has failed to comply with industry standards.

72. Because Defendant has failed to comply with industry standards, while monetary relief may cure some of Plaintiffs' and Class Members' injuries, injunctive relief is necessary to ensure Defendant's approach to information security is adequate and appropriate. Defendant still maintains the PHI of Plaintiffs and Class Members, and without the supervision of the Court via injunctive relief, Plaintiffs' and Class Members' PHI remains at risk of subsequent data breaches.

CLASS ACTION ALLEGATIONS

73. Plaintiffs bring this suit as a class action on behalf of themselves and on behalf of all others similarly situated pursuant to Rule 23(b)(2), (b)(3) and (c)(4) of the Federal Rules of Civil Procedure (the "Class Members").

74. The Nationwide Class that Plaintiffs seek to represent is defined as follows:

> All individuals in the United States who are current or former patients or customers of Defendant, whose PHI was compromised in the Data Breach (the "Class").

75. Excluded from the Class are the officers, directors, and legal representatives of Defendant, and the judges and court personnel in this case and any members of their immediate families.

76. Numerosity. Fed. R. Civ. P. 23(a)(1). The Class Members are so numerous that joinder of all Class Members is impractical. While the exact number of Class Members is unknown to Plaintiffs at this time, Defendant treated and serviced over 3.5 million patients in 2019 alone, and its nationwide servers were shut down as a result of the Data Breach. Therefore, based on information and belief, it is estimated that the Class numbers in the millions. The exact number is generally ascertainable by appropriate discovery as Defendant has knowledge of the customers/patients whose PHI was compromised in the Data Breach.

77. Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3). There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether and to what extent Defendant had a duty to protect the PHI of Class Members;

b. Whether Defendant was negligent in collecting and storing Plaintiffs' and Class Members' PHI;

c. Whether Defendant had respective duties not to disclose the PHI of Class Members to unauthorized third parties;

d. Whether Defendant had a duty to secure its networks in a manner so as to prevent interruption resulting in the cancelation, delay, and/or rescheduling of patients' medical procedures;

e. Whether Defendant took reasonable steps and measures to safeguard Plaintiffs' and

Class Members' PHI;

f. Whether Defendant failed to adequately safeguard the PHI of Plaintiffs and Class Members;

g. Whether Defendant breached its duty to exercise reasonable care in handling Plaintiffs' and Class Members' PHI by storing that information on computers susceptible to hacking by malicious actors;

h. Whether Defendant breached its duty to secure its networks in a manner so as to prevent interruption resulting in the cancelation, delay, and/or rescheduling or patients' medical procedures;

i. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

j. Whether implied or express contracts existed between Defendant, on the one hand, and Plaintiffs and Class Members on the other;

k. Whether Defendant had respective duties not to use the PHI of Class Members for non-business purposes;

l. Whether Defendant adequately and accurately informed Plaintiffs and Class Members that their PHI was subject to an unauthorized disclosure or access;

m. Whether Class Members are entitled to actual damages, statutory damages, and/or punitive damages as a result of Defendant's wrongful conduct;

a. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and,

b. Whether Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

78. Typicality. Fed. R. Civ. P. 23(a)(3). Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' PHI, like that of every other class Member, was disclosed by Defendant. Plaintiffs' claims are typical of those of the other Class Members because, *inter alia*, all Class Members were injured through the common misconduct of Defendant. Plaintiffs are advancing the same claims and legal theories on behalf of himself and all other Class Members, and there are no defenses that are unique to Plaintiffs. The claims of Plaintiffs and those of Class Members arise from the same operative facts and are based on the same legal theories.

79. Policies Generally Applicable to the Class. This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members, and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

80. Adequacy of Representation. Fed. R. Civ. P. 23(a)(4). Plaintiffs will fairly and adequately represent and protect the interests of the Class in that they have no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiffs seek no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiffs have retained counsel experienced in complex consumer class action litigation, and Plaintiffs intend to prosecute this action vigorously.

81. Superiority of Class Action. Fed. R. Civ. P. 23(b)(3). The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of class members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain class members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

82. The nature of this action and the nature of laws available to Plaintiffs and the Class make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and the Class for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

83. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class

Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

84. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

85. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PHI of Plaintiffs and Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

86. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

87. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiffs and the Class)

88. Plaintiffs restate and realleges paragraphs 1 through 87 above as if fully set forth herein.

89. As a condition of utilizing Defendant's services, customers/patients were obligated to provide Defendant with certain PHI, including their date of birth, mailing addresses, Social Security numbers, and personal medical information.

90. Plaintiffs and the Class Members entrusted their PHI to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PHI for

business purposes only, and/or not disclose their PHI to unauthorized third parties.

91. Defendant has full knowledge of the sensitivity of the PHI and the types of harm that Plaintiffs and Class Members could and would suffer if the PHI were wrongfully disclosed.

92. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using its customers/patients' PHI involved an unreasonable risk of harm to Plaintiffs and Class Members, even if the harm occurred through the criminal acts of a third party.

93. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that Plaintiffs' and Class Members' PHI in Defendant's possession was adequately secured and protected, and that employees tasked with maintaining such information were adequately trained on security measures regarding the security of customers/patients' PHI.

94. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiffs' and Class Members' PHI.

95. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Class Members was reasonably foreseeable, particularly in light of prior data breaches and disclosures prevalent in today's digital landscape.

96. Plaintiffs and the Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PHI of Plaintiffs and the Class, the critical importance of providing adequate security of that PHI, the necessity for encrypting PHI stored on Defendant's

systems, and that they had inadequate IT security protocols in place to secure the PHI of Plaintiffs and the Class.

97. Defendant's own conduct created a foreseeable risk of harm to Plaintiffs and Class Members. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included decisions not to comply with industry standards for the safekeeping and encrypted authorized disclosure of the PHI of Plaintiffs and Class Members.

98. Plaintiffs and the Class Members had no ability to protect their PHI that was in Defendant's possession.

99. Defendant was in a position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Breach.

100. Defendant has and continues to have a duty to adequately disclose that the PHI of Plaintiffs and Class Members within Defendant's possession might have been compromised, how it was compromised, and precisely the types of information that were compromised and when. Such notice is necessary to allow Plaintiffs and the Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PHI by third parties.

101. Defendant has a duty to employ proper procedures to prevent the unauthorized dissemination of the PHI of Plaintiffs and Class Members.

102. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiffs and Class Members by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PHI of Plaintiffs and Class Members during the time the PHI was within Defendant's possession or control.

103. Defendant improperly and inadequately safeguarded the PHI of Plaintiffs and Class

Members in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

104. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect its customers/patients' PHI in the face of increased risk of theft.

105. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of its customers/patients' PHI.

106. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and accurately disclose to Plaintiffs and Class Members the existence and scope of the Data Breach.

107. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and Class Members, the PHI of Plaintiffs and Class Members would not have been compromised.

108. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and Class Members, the procedures of Plaintiff Motkowicz and other patients of Defendant would not have been rescheduled, resulting in damages, including, *inter alia*, missed work, increased insurance costs, and pain and suffering.

109. There is a close causal connection between Defendant's failure to implement security measures to protect the PHI of current and former customers/patients and the harm suffered or risk of imminent harm suffered by Plaintiffs and the Class. Plaintiffs' and Class Members' PHI was accessed and compromised as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PHI by adopting, implementing, and maintaining appropriate security measures and encryption.

110. Similarly, there is a close causal connection between Defendant's failure to

implement security measures to ensure the continuity of its provision of medical services and the harm suffered by Plaintiff Motkowicz and the Class. Plaintiff Motkowicz's procedure was delayed, directly preventing him from returning to work and requiring him to procure alternative insurance.

111. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PHI. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

112. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PHI and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PHI it obtained and stored, and the foreseeable consequences of a Data Breach for companies of Defendant's magnitude, including, specifically, the immense damages that would result to Plaintiffs and Class Members.

113. Defendant's violations of Section 5 of the FTC Act constitute negligence *per se*.

114. Plaintiffs and Class Members are within the class of persons that the FTC Act was intended to protect.

115. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class Members.

116. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PHI is used; (iii) the compromise, publication, and/or theft of their PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery

from identity theft, tax fraud, and/or unauthorized use of their PHI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PHI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PHI of customers/patients and former customers/patients in its continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; (ix) the diminished value of Defendant's goods and services they received; (x) lost wages; (xi) increased costs of insurance; and (xii) pain and suffering.

117. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

SECOND CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiffs and the Class)

118. Plaintiffs restate and reallege paragraphs 1 through 87 above as if fully set forth herein.

119. Plaintiffs and Class Members were required to provide their PHI, including names, addresses, Social Security numbers, dates of birth, and other personal information, to Defendant as a condition of their use of Defendant's services.

120. Plaintiffs and Class Members paid money to Defendant in exchange for goods and services, as well as Defendant's promises to protect their PHI from unauthorized disclosure.

121. In its written privacy policy, Defendant expressly promised Plaintiffs and Class Members that Defendant would only disclose PHI under certain circumstances, none of which relate to the Data Breach.

122. Defendant promised to comply with HIPAA standards and to make sure that Plaintiffs' and Class Members' PHI would remain protected.

123. Implicit in the agreement between the Defendant's customers/patients, including Plaintiffs and Class Members, to provide PHI, and Defendant acceptance of such PHI, was Defendant's obligation to use the PHI of its customers/patients for business purposes only, take reasonable steps to secure and safeguard that PHI, and not make unauthorized disclosures of the PHI to unauthorized third parties.

124. Further, implicit in the agreement, Defendant was obligated to provide Plaintiffs and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PHI.

125. Without such implied contracts, Plaintiffs and Class Members would not have provided their PHI to Defendant.

126. Defendant had an implied duty to reasonably safeguard and protect the PHI of Plaintiffs and Class Members from unauthorized disclosure or uses.

127. Additionally, Defendant implicitly promised to retain this PHI only under conditions that kept such information secure and confidential.

128. Plaintiffs and Class Members fully performed their obligations under the implied contract with Defendant; however, Defendant did not.

129. Defendant breached the implied contracts with Plaintiffs and Class Members by failing to reasonably safeguard and protect Plaintiffs' and Class Members' PHI, which was compromised as a result of the Data Breach.

130. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to comply with its promise to abide by HIPAA.

131. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to ensure the confidentiality and integrity of electronic protected health information Defendant created, received, maintained, and transmitted in violation of 45 CFR 164.306(a)(1).

132. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1).

133. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1).

134. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 CFR 164.308(a)(6)(ii).

135. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2).

136. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 CFR 164.306(a)(3).

137. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce violations in violation of 45 CFR 164.306(a)(94).

138. Defendant further breached the implied contracts with Plaintiffs and Class Members by impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 CFR 164.502, *et seq*.

139. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to effectively train all members of its workforce (including independent contractors) on the policies and procedures with respect to protected health information as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of protected health information in violation of 45 CFR 164.530(b) and 45 CFR 164.308(a)(5).

140. Defendant further breached the implied contracts with Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' PHI.

141. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to maintain a safe and secure network environment to ensure the procedures of Plaintiff Motkowicz and others would not have been rescheduled, resulting in damages, including, *inter alia*, missed work, increased insurance costs, and pain and suffering.

142. Defendant's failures to meet these promises constitute breaches of the implied

contracts.

143. Because Defendant allowed unauthorized access to Plaintiffs' and Class Members' PHI and failed to safeguard the PHI, Defendant breached its contracts with Plaintiffs and Class Members.

144. A meeting of the minds occurred, as Plaintiffs and Class Members agreed, *inter alia*, to provide accurate and complete PHI and to pay Defendant in exchange for Defendant's agreement to, *inter alia*, protect their PHI.

145. Defendant breached its contracts with Plaintiffs and Class Members by not meeting the minimum level of protection of Plaintiffs' and Class Members' PHI, because it did not prevent against the Data Breach.

146. Furthermore, the failure to meet its confidentiality and privacy obligations resulted in Defendant providing goods and services to Plaintiffs and Class Members that were of a diminished value.

147. As a direct and proximate result of Defendant's breach of its implied contracts with Plaintiffs and Class Members, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PHI is used; (iii) the compromise, publication, and/or theft of their PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PHI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PHI, which remain in Defendant's possession and is

subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PHI of customers/patients and former customers/patients in its continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; (ix) the diminished value of Defendant's goods and services they received; (x) lost wages; (xi) increased costs of insurance; and (xii) pain and suffering.

148. As a direct and proximate result of Defendant's breach of its implied contracts with Plaintiffs and Class Members, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

THIRD CAUSE OF ACTION
Breach of Fiduciary Duty
(On Behalf of Plaintiffs and the Class)

149. Plaintiffs restate and reallege paragraphs 1 through 87 above as if fully set forth herein.

150. In light of the special relationship between Defendant and its customers/patients, whereby Defendant became guardians of Plaintiffs' and Class Members' highly sensitive, confidential, and personal PHI, Defendant was a fiduciary, created by its undertaking and guardianship of the PHI, to act primarily for the benefit of its customers/patients, including Plaintiffs and Class Members, for: 1) the safeguarding of Plaintiffs and Class Members' PHI; 2) to timely notify Plaintiffs' and Class Members' of a data breach or disclosure; and 3) maintain complete and accurate records of what and where Defendant's customers/patients' information was and is stored.

151. Defendant had a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of its customers/patients' relationship, in particular to keep secure the PHI of its customers/patients and to maintain the security of its networks so as to ensure continuity of its provision of medical services.

152. Defendant breached its fiduciary duty to Plaintiffs and Class Members by failing to encrypt and otherwise protect Plaintiffs' and Class Members' PHI.

153. Defendant breached its fiduciary duty to Plaintiff Motkowicz and the Class by failing to implement network security sufficient to ensure continuity of its provision of medical services.

154. Defendant breached its fiduciary duty to Plaintiffs and Class Members by failing to timely notify and/or warn Plaintiffs and Class Members of the Data Breach.

155. Defendant breached its fiduciary duty to Plaintiffs and Class Members by failing to ensure the confidentiality and integrity of electronic protected health information Defendant created, received, maintained, and transmitted, in violation of 45 CFR 164.306(a)(1).

156. Defendant breached its fiduciary duty to Plaintiffs and Class Members by failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1).

157. Defendant breached its fiduciary duty to Plaintiffs and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 CFR 164.308(a)(1).

158. Defendant breached its fiduciary duty to Plaintiffs and Class Members by failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable,

harmful effects of security incidents that are known to the covered entity in violation of 45 CFR 164.308(a)(6)(ii).

159. Defendant breached its fiduciary duty to Plaintiffs and Class Members by failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2).

160. Defendant breached its fiduciary duty to Plaintiffs and Class Members by failing to protect against any reasonably-anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 CFR 164.306(a)(3).

161. Defendant breached its fiduciary duty to Plaintiffs and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce in violation of 45 CFR 164.306(a)(94).

162. Defendant breached its fiduciary duty to Plaintiffs and Class Members by impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 CFR 164.502, *et seq.*

163. Defendant breached its fiduciary duty to Plaintiffs and Class Members by failing to effectively train all members of its workforce (including independent contractors) on the policies and procedures with respect to protected health information as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of protected health information in violation of 45 CFR 164.530(b) and 45 CFR 164.308(a)(5).

164. Defendant breached its fiduciary duty to Plaintiffs and Class Members by failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard protected health information, in compliance with 45 CFR

164.530(c).

165. Defendant breached its fiduciary duty to Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' PHI.

166. As a direct and proximate result of Defendant's breach of its implied contracts with Plaintiffs and Class Members, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PHI is used; (iii) the compromise, publication, and/or theft of their PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PHI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PHI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PHI of customers/patients and former customers/patients in its continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; (ix) the diminished value of Defendant's goods and services they received; (x) lost wages; (xi) increased costs of insurance; and (xii) pain and suffering.

167. As a direct and proximate result of Defendant's breaches of its fiduciary duty, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic

and non-economic losses.

FOURTH CAUSE OF ACTION
Breach of Confidence
(On Behalf of Plaintiffs and the Class)

168. Plaintiffs restate and reallege paragraphs 1 through 87 above as if fully set forth herein.

169. At all times during Plaintiffs' and Class Members' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiffs' and Class Members' PHI that Plaintiffs and Class Members provided to Defendant.

170. As alleged herein and above, Defendant's relationship with Plaintiffs and Class Members was governed by terms and expectations that Plaintiffs' and Class Members' PHI would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

171. Plaintiffs and Class Members provided their respective PHI to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the PHI to be disseminated to any unauthorized third parties.

172. Plaintiffs and Class Members also provided their respective PHI to Defendant with the explicit and implicit understandings that Defendant would take precautions to protect that PHI from unauthorized disclosure.

173. Defendant voluntarily received in confidence Plaintiffs' and Class Members' PHI with the understanding that PHI would not be disclosed or disseminated to the public or any unauthorized third parties.

174. Due to Defendant's failure to prevent, detect, and avoid the Data Breach from occurring, Plaintiffs' and Class Members' PHI was disclosed and misappropriated to unauthorized

third parties beyond Plaintiffs' and Class Members' confidence, and without their express permission.

175. Due to Defendant's failure to prevent, detect, and avoid the Data Breach from occurring, the procedures of Plaintiff Motkowicz and the Class would not have been rescheduled, resulting in damages, including, *inter alia*, missed work, increased insurance costs, and pain and suffering.

176. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiffs and Class Members have suffered damages.

177. Similarly, as a direct and proximate cause of Defendant's actions and/or omissions to ensure the continuity of its provision of medical services, Plaintiff Motkowicz's procedure was delayed, directly preventing him from returning to work and requiring him to procedure additional insurance.

178. But for Defendant's disclosure of Plaintiffs' and Class Members' PHI in violation of the parties' understanding of confidence, their PHI would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiffs' and Class Members' PHI, as well as the resulting damages.

179. But for Defendant's failure to maintain sufficient network security, Plaintiff Motkowicz and other Class Members would not have had their procedures delayed, and would have been able to return to work and not procure additional insurance.

180. The injury and harm Plaintiffs and Class Members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiffs' and Class Members' PHI. Defendant knew or should have known its computer systems and technologies for accepting and securing Plaintiffs' and Class Members' PHI had numerous security vulnerabilities.

181. As a direct and proximate result of Defendant's breach of its implied contracts with Plaintiffs and Class Members, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PHI is used; (iii) the compromise, publication, and/or theft of their PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PHI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PHI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PHI of customers/patients and former customers/patients in its continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; (ix) the diminished value of Defendant's goods and services they received; (x) lost wages; (xi) increased costs of insurance; and (xii) pain and suffering.

182. As a direct and proximate result of Defendant's breaches of confidence, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

PRAYER FOR RELIEF

WHEREFORE Plaintiffs on behalf of themselves and all others similarly situated, pray for relief as follows:

a. For an Order certifying the Class as defined herein, and appointing Plaintiffs and their Counsel to represent the Class;

b. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and the Class Members' PHI;

c. For equitable relief compelling Defendant to use appropriate cyber security methods and policies with respect to PHI collection, storage, and protection, and to disclose with specificity to Class Members the type of PHI compromised;

d. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

e. For an award of punitive damages;

f. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

g. For prejudgment interest on all amounts awarded; and

h. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury on all issues so triable.

Dated: January 8, 2021

Respectfully submitted,

/s/ *John A. Yanchunis*

JOHN A. YANCHUNIS (*pro hac vice*)
jyanchunis@ForThePeople.com
RYAN J. MCGEE (*pro hac vice*)
rmcgee@ForThePeople.com
MORGAN & MORGAN

COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 223-5505
Facsimile: (813) 223-5402

KEVIN CLANCY BOYLAN (PA ID: 317114)
kboylan@forthepeople.com
1800 JFK BLVD., Suite 1400
Philadelphia, PA 19103
Telephone: (215) 446-9795
Fax: (215) 446-9799

William 'Billy' Peerce Howard
Billy@TheConsumerProtectionFirm.com
THE CONSUMER PROTECTION FIRM
4030 Henderson Boulevard
Tampa, FL 33629
(813) 500-1500 Telephone
(813) 435-2369 Facsimile

Attorneys for Plaintiffs and the Proposed Class